REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-18 are presently active, and Claims 1-3, 6-9, 13, 15, 16 and 18 are amended to clarify the subject matter. No new matter is added.

In the outstanding Office Action, Claim 18 was rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter; Claims 1, 3-7, 13 and 18 were rejected under 35 U.S.C. § 102(e) as anticipated by Matsuyama (U.S. Pat. Application Pub. No. 2004/0078573); and Claims 2, 8-12 and 14-17 were rejected under 35 U.S.C. § 103(a) as unpatentable over Matsuyama in view of Barrett et al. (U.S. Pat. Application Pub. No. 2005/0160161).

Regarding the 35 U.S.C. § 101 rejection of Claim 18, the outstanding Office Action states that "page 27, lines 21-25 defined the recording medium as being CD-ROM, a magnetic disk, or a semiconductor storage device, ***or a communication line***. The Office's current position is that claims involving ***signals (i.e., communication line)*** encoded with functional descriptive material do not fall within any of the categories of patentable subject matter ... " (Office Action at page 2, paragraph 2, emphasis added).

However, the specification at page 27, lines 21-25 only describes that "the packet cryptographic processing substitution program can be ... downloaded to the computer via communication line into the computer, ... ," and does not define the recording medium as being a communication line. Instead, the specification at page 27, lines 21-25 describes that the packet cryptographic processing substitution program can be installed in the computer from a recording medium such as a CD-ROM, a magnetic disk and a semiconductor storage device.

Thus, Claim 18 does not involve signals (i.e., communication line), and therefore, Applicants respectfully request withdrawal of the 35 U.S.C. § 101 rejection.

Regarding the rejection under 35 U.S.C. § 102(e) and § 103(a), Applicants respectfully submit that the rejection is overcome because, in Applicants' view, independent Claims 1 and 13 patentably distinguish over the applied references as discussed below.

Claim 1 recites, *inter alia*, "cryptographic processing part which performs ***cryptographic processing*** for a received packet which is forwarded from the counterpart apparatus to the terminal or from the terminal to the counterpart apparatus, based on the cryptographic communication channel information stored in said cryptographic communication channel information storage part."

Instead, Matsuyama describes that the home gateway 20 includes, for example, the concept of home routers, firewalls, and/or bridges, corresponds to a network gate which allows networks having different protocols to be connected, and functions as an interface for mutually connecting the home network to which the target units 10_1 and 10_2 belong and another network (Matsuyama at paragraph 0073, lines 2-8). The home gateway 20 holds the public-key ***certificate*** PKC_G issued by the certification authority CA, and uses the public-key ***certificate*** PKC_G to perform ***mutual authentication*** with the target units 10_1 and 10_2, the portable unit 30, and the attribute authority AA (Matsuyama at paragraph 0073, lines 8-12). That is, the home gateway 20 only functions as an interface for the mutual connection and performs the mutual authentication using the public-key certification. Matsuyama does not teach or even suggest that the home gateway 20 performs ***cryptographic processing*** for a received packet which is forwarded from the counterpart apparatus to the terminal or from the terminal to the counterpart apparatus.

Thus, Matsuyama fails to teach at least "cryptographic processing part which performs cryptographic processing for a received packet which is forwarded from the

counterpart apparatus to the terminal or from the terminal to the counterpart apparatus, based on the cryptographic communication channel information stored in said cryptographic communication channel information storage part," as recited in Claim 1.

Since similar arguments as set forth above apply to Claim 13, Matsuyama fails to teach at least "(b) performing cryptographic processing for a received packet which is forwarded from the counterpart apparatus to the terminal or from the terminal to the counterpart apparatus, based on the cryptographic communication channel information," as recited in Claim 13.

Accordingly, independent Claims 1 and 13 patentably distinguish over the applied references. Since Claims 2-12 and 14-18 are dependent directly or indirectly from Claims 1 and 13, substantially the same arguments set forth above also apply to these dependent claims. Therefore, Claims 1-18 are believed to be allowable.

Last, Applicants note that some of the dependent claims clearly distinguish over the applied references as below.

Claim 3 recites "a received packet determination part which determines ***whether or not a received packet*** from the counterpart apparatus which is forwarded to the terminal ***is valid***."

However, Matsuyama only describes performing mutual authentication ***with the target units 10_1 and 10_2*** by using the public-key certificate PKC_G (Matsuyama at paragraph 0073, lines 8-12). That is, what the home gateway 20 in Matsuyama certifies is the content of the attribute certificate AC_P, not a received packet.

Thus, Matsuyama fails to teach or even suggest "a received packet determination part which determines ***whether or not a received packet*** from the counterpart apparatus which is forwarded to the terminal ***is valid***," as recited in Claim 3.

Regarding Claim 4, the outstanding Office Action indicates that the block CA in Matsuyama corresponds to "a detachable, tamper-proof device" as recited in Claim 4 (Office Action at page 4, paragraph 10).

However, the block CA is the entity which issues the public-key certifications PKC_{T2}, PKC_G and PKC_M (Matsuyama at paragraph 0051) and not a detachable, tamper-proof device in which at least part of the cryptographic communication channel information is stored.

Thus, Matsuyama fails to teach or even suggest "said cryptographic communication channel information storage part includes a detachable, tamper-proof device in which at least part of the cryptographic communication channel information is stored," as recited in Claim 4.

Regarding Claim 5, the outstanding Office Action indicates that the attribute authority in Matsuyama corresponds to "a storage medium" as recited in Claim 5.

However, Matsuyama does not teach or even suggest that the attribute authority AA updates the attribute certificate. Instead, the attribute authority AA only issues the attribute certificates AC_{LI}, AC_{PI} and AC_H (Matsuyama in Fig. 17, step S42).

Thus, Matsuyama fails to teach or even suggest "said cryptographic communication channel information storage part includes a storage medium in which at least part of the cryptographic communication channel information is changeable," as recited in Claim 5.

Claim 7 is amended to clarify that the claimed device on which the packet cryptographic processing proxy apparatus is implemented has no IP address.

Instead, the outstanding Office Action states that the home gateway 20 in Matsuyama has at least two IP addresses.

Thus, Claim 7 clearly patentably distinguishes over Matsuyama.

Regarding Claim 8, the outstanding Office Action states that Barrett et al. discloses the filter information and storing the information in the filter information storage part (Office Action at page 6, paragraph 20).

However, Barrett et al. at paragraph 0032 only describes that an access server 106 may include a variety of packet filter, proxy applications and screening applications to determine if a packet is authorized.

Thus, Barrett et al. fails to teach or even suggest the features as recited in Claim 8.

Claim 9 recites a packet determination part, a cryptographic communication channel information agreement part and a key information setting part.

The outstanding Office Action states that Matsuyama in Figs. 13 (step S15) and 18 (step S 56) and at paragraphs 0101 and 0151 teaches a packet determination part as recited in Claim 9 (Office Action at page 7, lines 1-5).

However, Matsuyama in Figs. 13 (step S15) and 18 (step S56) and at paragraphs 0101 and 0151 only describes that the target units 10_1, 10_2 (10_3) verify the contents of the attribute certificates AC_P (AC_{P1}, AC_H).

Thus, Matsuyama fails to teach or even suggest a packet determination part as recited in Claim 9.

Further, the outstanding Office Action states that Matsuyama in Figs. 13 (block S16) and 18 (block S57) and at paragraphs 0101 and 0151 teaches a cryptographic communication channel information agreement part as recited in Claim 9 (Office Action at page 7, lines 6-9).

However, Matsuyama in Figs. 13 (block S16) and 18 (block S57) and at paragraphs 0101 and 0151 only describes that the target units 10_1, 10_2 (10_3) permit accessing from the portable unit 30 (30_1).

Thus, Matsuyama fails to teach or even suggest a cryptographic communication channel information agreement part as recited in Claim 9.

Further, the outstanding Office Action states that Barrett et al. at paragraph 0067 teaches a client device setting an encryption key to be used for secure communications (Office Action at page 7, lines 14-15).

However, Barrett et al. at paragraph 0067 only describes that the client which sends a security attribute includes at least an encryption key.

Thus, Barrett et al. fails to teach or even suggest a key information setting part as recited in Claim 9.

Regarding Claim 10, the outstanding Office Action states that Matsuyama in Figs. 13 (blocks S15, S16) and 18 (blocks S57, S58) and at paragraphs 0101 and 0151 teaches the features as recited in Claim 10.

However, Matsuyama in Figs. 13 (blocks S15, S16) and 18 (blocks S57, S58) and at paragraphs 0101 and 0151 only describes that: the target units 10_1, 10_2 (10_3) verify the contents of the attribute certificates AC_P (AC_{P1}', AC_H); if the verification result is affirmative, the target units 10_1, 10_2 (10_3) permit accessing from the portable unit 30 (30_1); and if the verification result is not affirmative, the target units 10_1, 10_2 (10_3) do not permit accessing from the portable unit 30 (30_1).

Thus, Matsuyama fails to teach or even suggest the features as recited in Claim 10.

Regarding Claim 11, the outstanding Office Action states that Barrett et al. at paragraph 0067 teaches the features as recited in Claim 11 (Office Action at page 8, paragraph 26).

However, it is respectfully submitted that Barrett et al. at paragraph 0067 does not teach or even suggest anything about the features as recited in Claim 11.

Regarding Claim 12, the outstanding Office Action states that Barrett et al. at paragraph 0032 teaches the features as recited in Claim 12 (Office Action at pages 8-9, paragraph 27).

However, it is respectfully submitted that Barrett et al. at paragraph 0032 does not teach or even suggest anything about the features as recited in Claim 12.

Regarding Claim 15, the outstanding Office Action states that Barrett et al. at paragraph 0067 teaches a client device and a proxy device negotiating and setting a secure communication session, using an encryption key to be used for secure communications (Office Action at page 10, paragraph 32).

However, Barrett et al. does not teach that setting the key information allows the secure connection with inherited authentification and authorization attributes, which create a relatively simple method for establishing a secure connection with a proxy (see Barrett et al. at paragraphs 0001 and 0007).

Thus, Barrett et al. fails to teach or even suggest the features as recited in Claim 15.

Regarding Claim 16, the outstanding Office Action indicates that Matsuyama in Figs. 13 (blocks S16, S17) and 18 (blocks S57, S58) and at paragraphs 0101 and 0151 teaches the claimed step (a-1-1), and Barrett et al. at paragraph 0067 teaches the claimed step (a-1-2) (Office Action at page 11, paragraphs 34 and 35).

However, Matsuyama in Figs. 13 (blocks S16, S17) and 18 (blocks S57, S58) and at paragraphs 0101 and 0151 only describes that: the target units 10_1, 10_2 (10_3) verify the contents of the attribute certificates AC_P ($AC_{P1'}$, AC_H); if the verification result is affirmative, the target units 10_1, 10_2 (10_3) permit accessing from the portable unit 30 (30_1); and if the verification result is not affirmative, the target units 10_1, 10_2 (10_3) do not permit accessing from the portable unit 30 (30_1).

Thus, Matsuyama fails to teach or even suggest the claimed step (a-1-1).

Further, Barrett et al. at paragraph 0067 only describes that the client which sends a security attribute includes at least an encryption key.

Thus, Barrett et al. fails to teach or even suggest the claimed step (a-1-2).

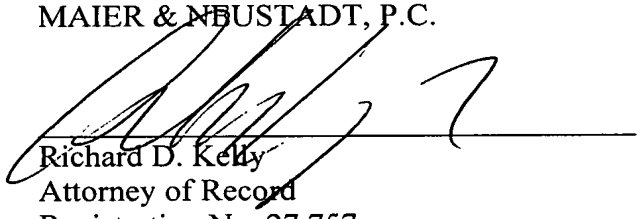
Regarding Claim 17, the outstanding Office Action indicates that Barrett et al. at paragraph 0032 teaches the claimed features (Office Action at page 11, paragraph 36).

However, it is respectfully submitted that Barrett et al. at paragraph 0032 does not teach or even suggest anything about the features as recited in Claim 17.

In view of the amendments and discussions presented above, Applicants respectfully submit that the present application is in condition for allowance, and an early action favorable to that effect is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Richard D. Kelly
Attorney of Record
Registration No. 27,757

Akihiro Yamazaki
Registration No. 46,155

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

RDK/AY/TY:pta
I:\ATTY\TY\AMEND-RESPONSES\277747\277747 AM DUE JULY 30 2007.DOC